

# On the Complexity of Hilbert Refutations for Partition

S. Margulies

*Department of Mathematics, Pennsylvania State University, State College, PA*

S. Onn<sup>1</sup>

*Industrial Engineering & Management, Technion - Israel Institute of Technology, Haifa, Israel*

---

## Abstract

Given a set of integers  $W$ , the PARTITION problem determines whether  $W$  can be divided into two disjoint subsets with equal sums. We model the PARTITION problem as a system of polynomial equations, and then investigate the complexity of a Hilbert's Nullstellensatz refutation, or certificate, that a given set of integers is not partitionable. We provide an explicit construction of a minimum-degree certificate, and then demonstrate that the PARTITION problem is equivalent to the determinant of a carefully constructed matrix called the partition matrix. In particular, we show that the determinant of the partition matrix is a polynomial that factors into an iteration over all possible partitions of  $W$ .

*Key words:* Hilbert's Nullstellensatz, linear algebra, partition

---

## 1. Introduction

The NP-complete problem PARTITION (9) is the question of deciding whether or not a given set of integers  $W = \{w_1, \dots, w_n\}$  can be broken into two sets,  $I$  and  $W \setminus I$ , such that the sums of the two sets are equal, or that  $\sum_{w \in I} w = \sum_{w \in W \setminus I} w$ . Since it is widely believed that  $\text{NP} \neq \text{coNP}$ , it is interesting to study various types of *refutations*, or certificates for the *non*-existence of a partition in a given set  $W$ .

In this paper, we study the certificates provided by Hilbert's Nullstellensatz (see (1; 2; 8; 10; 12) and references therein). Given an algebraically-closed field  $\mathbb{K}$  and a set of polynomials  $f_1, \dots, f_s \in \mathbb{K}[x_1, \dots, x_n]$ , Hilbert's Nullstellensatz states that the system of polynomial equations  $f_1 = f_2 = \dots = f_s = 0$  has *no* solution if and only if there exist polynomials  $\beta_1, \dots, \beta_s \in \mathbb{K}[x_1, \dots, x_n]$  such that  $1 = \sum_{i=1}^s \beta_i f_i$ . We measure the complexity of a given certificate in terms of the size of the  $\beta$  coefficients, since these are

---

*Email addresses:* `margulies@math.psu.edu` (S. Margulies), `onn@ie.technion.ac.il` (S. Onn).

<sup>1</sup> Research of this author was supported in part by a grant from the Israel Science Foundation.

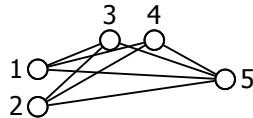
the unknowns we must discover in order to demonstrate the *non*-existence of a solution to  $f_1 = f_2 = \dots = f_s = 0$ . Thus, we measure the degree of a Nullstellensatz certificate as  $d = \max\{\deg(\beta_1), \dots, \deg(\beta_s)\}$ .

There is a well-known connection between Hilbert's Nullstellensatz and a particular sequence of linear algebra computations. These sequences have been studied from both a theoretical perspective (4; 8), and a computational perspective (7; 6). In (4), Buss and Pitassi show that a polynomial system loosely based upon the “pigeon-hole principle” requires a  $\lfloor \log n \rfloor - 1$  Nullstellensatz degree certificate. However, when the system of polynomial equations  $f_1, \dots, f_s$  models an NP-complete problem, the degree  $d$  is likely to grow at least linearly with the size of the underlying NP-complete instance (11). In other words, as long as  $P \neq NP$ , the certificates should be hard to find (i.e., the size of the linear systems involved should be exponential in the size of the underlying instance), and as long as  $NP \neq coNP$ , the certificates should be hard to verify (i.e., the certificates should contain an exponential number of monomials).

For example, consider the NP-complete problem of finding an independent set of size  $k$  in a graph  $G$ . Recall that an independent set is a set of pairwise non-adjacent vertices. This problem was modeled by Lovász (10) as a system of polynomial equations as follows:

$$\begin{aligned} x_i^2 - x_i &= 0, \text{ for every vertex } i \in V(G), \\ x_i x_j &= 0, \text{ for every edge } (i, j) \in E(G), \\ -k + \sum_{i=1}^n x_i &= 0. \end{aligned}$$

Clearly, this system of polynomial equations has a solution if and only if the underlying graph  $G$  has an independent set of size  $k$ . For example, consider the Turán graph  $T(5, 3)$ :



By inspection, we see that size of the largest independent set in  $T(5, 3)$  is two. Therefore, there is *no* independent set of size three, and using the connection between Hilbert's Nullstellensatz and linear algebra (described more thoroughly in Sec 3), the authors of (8) produce the following certificate:

$$\begin{aligned} 1 &= \underbrace{\left( -\frac{1}{3}(x_1 x_2 + x_3 x_4) - \frac{1}{6}(x_1 + x_2 + x_3 + x_4 + x_5) - \frac{1}{3} \right)}_{\beta_1} (x_1 + x_2 + x_3 + x_4 + x_5 - 3) + \\ &\quad \left( \frac{1}{3}x_4 + \frac{1}{3}x_2 + \frac{1}{3} \right) x_1 x_3 + \left( \frac{1}{3}x_2 + \frac{1}{3} \right) x_1 x_4 + \left( \frac{1}{3}x_2 + \frac{1}{3} \right) x_1 x_5 + \left( \frac{1}{3}x_4 + \frac{1}{3} \right) x_2 x_3 + \\ &\quad \left( \frac{1}{3} \right) x_2 x_4 + \left( \frac{1}{3} \right) x_2 x_5 + \left( \frac{1}{3}x_4 + \frac{1}{3} \right) x_3 x_5 + \left( \frac{1}{3} \right) x_4 x_5 + \left( \frac{1}{3}x_2 + \frac{1}{6} \right) (x_1^2 - x_1) + \\ &\quad \left( \frac{1}{3}x_1 + \frac{1}{6} \right) (x_2^2 - x_2) + \left( \frac{1}{3}x_4 + \frac{1}{6} \right) (x_3^2 - x_3) + \left( \frac{1}{3}x_3 + \frac{1}{6} \right) (x_4^2 - x_4) + \left( \frac{1}{6} \right) (x_5^2 - x_5). \end{aligned}$$

The combinatorial interpretation of this algebraic identity is unexpectedly clear: the size of the largest independent set is the degree of the Nullstellensatz certificate (i.e., the largest monomial  $x_1 x_2$  corresponds to the maximum independent set formed by vertices  $\{1, 2\}$ ), and the coefficient  $\beta_1$  contains one monomial for each independent set in  $G$ . The combinatorial interpretation of these certificates is proven in (8) by De Loera et al. only in terms of monomials: the relationship between the numbers such as  $1/3$  and  $1/6$  and the independent sets of the underlying graph is not clear.

In this paper, we model the PARTITION problem as a system of polynomial equations, and then present a combinatorial interpretation of an associated minimum-degree Nullstellensatz certificate. However, the focus of our combinatorial interpretation is not only on the relationship between partitions and monomials, but also on the relationship between partitions and numeric coefficients (i.e., the numbers  $1/3$  and  $1/6$ ). In Section 2, we present an algebraic model of the partition problem and describe a minimum-degree Nullstellensatz certificate. In Section 3, we describe the connection between Hilbert's Nullstellensatz and linear algebra, leading to the construction of a *square* system of linear equations, forming what we call the *partition matrix*. In Section 4, we prove our main result: the determinant of the partition matrix represents a brute-force iteration over *all* the possible partitions of the set  $W$ , a polynomial we refer to as the *partition polynomial*.

We conclude our introduction with an example. Let  $W = \{w_1, w_2, w_3, w_4\}$ , and we see that the determinant of associated *partition matrix* is as follows:

$$\det \begin{pmatrix} w_4 & w_3 & w_2 & w_1 & 0 & 0 & 0 & 0 \\ w_3 & w_4 & 0 & 0 & w_2 & w_1 & 0 & 0 \\ w_2 & 0 & w_4 & 0 & w_3 & 0 & w_1 & 0 \\ w_1 & 0 & 0 & w_4 & 0 & w_3 & w_2 & 0 \\ 0 & w_2 & w_3 & 0 & w_4 & 0 & 0 & w_1 \\ 0 & w_1 & 0 & w_3 & 0 & w_4 & 0 & w_2 \\ 0 & 0 & w_1 & w_2 & 0 & 0 & w_4 & w_3 \\ 0 & 0 & 0 & 0 & w_1 & w_2 & w_3 & w_4 \end{pmatrix} = \begin{aligned} & (w_1 + w_2 + w_3 + w_4)(-w_1 + w_2 + w_3 + w_4) \\ & (w_1 - w_2 + w_3 + w_4)(w_1 + w_2 - w_3 + w_4) \\ & (-w_1 + w_2 - w_3 + w_4)(-w_1 - w_2 + w_3 + w_4) \\ & (w_1 - w_2 - w_3 + w_4)(-w_1 - w_2 - w_3 + w_4) . \end{aligned}$$

Thus, the determinant of the *partition matrix* does indeed factor into a brute-force iteration of every possible partition of  $W$ : the *partition polynomial*.

## 2. Partitions and a System of Polynomial Equations

The PARTITION problem determines if a given set of integers  $W = \{w_1, \dots, w_n\}$  can be divided into two sets,  $I$  and  $W \setminus I$  such that  $\sum_{w \in I} w = \sum_{w \in W \setminus I} w$ . In this section, we describe a system of polynomial equations that models this question, and discuss the degree and monomials in an associated minimum-degree Nullstellensatz certificate.

**Proposition 1.** *Given a set of integers  $W = \{w_1, \dots, w_n\}$ , the following system of polynomial equations*

$$\begin{aligned} x_i^2 - 1 &= 0, \quad \text{for } 1 \leq i \leq n, \\ \sum_{i=1}^n w_i x_i &= 0. \end{aligned}$$

*has a solution if and only if there exists a partition of  $W$  into two sets,  $I \subseteq W$  and  $W \setminus I$ , such that  $\sum_{w \in I} w = \sum_{w \in W \setminus I} w$ .*

*Proof:* The variables  $x_i$  can take on the values of  $\pm 1$ . Thus, we relate partitions to solutions by placing integers  $w_i$  with  $+1$   $x_i$  values on one side of the partition and integers  $w_i$  with  $-1$   $x_i$  values on the other.  $\square$

Let  $[n]$  denote the set of integers  $\{1, \dots, n\}$  and let  $S_k^n$  denote the set of  $k$ -subsets of  $[n]$ . For  $S \in S_k^n$ , let  $x^S$  denote the corresponding square-free monomial of degree  $k$  in  $n$  variables. For example, given  $S = \{1, 3, 4\} \subseteq [5]$ , the corresponding monomial  $x^S = x_1 x_3 x_4$ . Additionally, let  $S_k^{n \setminus i}$  denote the  $k$ -subsets of  $[n] \setminus i$ .

**Theorem 2.** *Given a set of non-partitionable integers  $W = \{w_1, \dots, w_n\}$  encoded as a system of polynomial equations according to Prop. 1, there exists a minimum-degree Nullstellensatz certificate for the non-existence of a partition of  $W$  as follows:*

$$1 = \sum_{i=1}^n \left( \sum_{\substack{k \text{ even} \\ k \leq n-1}} \sum_{S \in S_k^{n \setminus i}} c_{i,S} x^S \right) (x_i^2 - 1) + \left( \sum_{\substack{k \text{ odd} \\ k \leq n}} \sum_{S \in S_k^n} b_S x^S \right) \left( \sum_{i=1}^n w_i x_i \right).$$

Moreover, every Nullstellensatz certificate for the system of equations defined by Prop. 1 contains one monomial for each of the odd parity subsets of each  $S_k^n$ , and one monomial for each of the even parity subsets of each  $S_k^{n \setminus i}$ .

Via Thm. 2, we see that the degree of the certificate is  $n$  for  $n$  odd, and  $n - 1$  for  $n$  even. Furthermore, by considering the monomials present in the certificate as identifying the integers present on *one* side of a partition, we see that the monomials represent a brute-force iteration over every possible partition of  $W$ . We note that we identify the constant terms  $c_{i,\emptyset}$  with the case of placing every integer on one side of the partition and the empty set on the other. Thus, this result is similar to the independent set result (De Loera et al., (8)) reviewed in the introduction. However, in this paper, we are interested not only in a combinatorial interpretation of the monomials, but also in a combinatorial interpretation of the unknowns  $c_{i,S}, b_S$ .

The proof of Thm. 2 is virtually identical to the proof of the independent set result described in (8). Thus, we omit the formal proof here and state only the result: the Nullstellensatz certificates associated with this simple formulation of the NP-complete PARTITION problem are both hard to find and hard to verify.

**Example 1.** *The set of integers  $W = \{1, 3, 5, 2\}$  is not partitionable. We encode this problem as a system of polynomial equations as follows:*

$$x_1^2 - 1 = 0, \quad x_2^2 - 1 = 0, \quad x_3^2 - 1 = 0, \quad x_4^2 - 1 = 0, \quad x_1 + 3x_2 + 5x_3 + 2x_4 = 0.$$

Since  $W$  is not partitionable, this system of equations has no solution, and a Nullstellensatz certificate exists. Here is the minimum-degree certificate described by Thm. 2:

$$\begin{aligned} 1 = & \left( -\frac{155}{693} + \frac{842}{3465}x_2x_3 - \frac{188}{693}x_2x_4 + \frac{908}{3465}x_3x_4 \right) (x_1^2 - 1) + \left( -\frac{1}{231} + \frac{842}{1155}x_1x_3 - \frac{188}{231}x_1x_4 \right. \\ & + \left. \frac{292}{1155}x_3x_4 \right) (x_2^2 - 1) + \left( -\frac{467}{693} + \frac{842}{693}x_1x_2 + \frac{908}{693}x_1x_4 + \frac{292}{693}x_2x_4 \right) (x_3^2 - 1) + \left( -\frac{68}{693} - \frac{376}{693}x_1x_2 \right. \\ & + \left. \frac{1816}{3465}x_1x_3 + \frac{584}{3465}x_2x_3 \right) (x_4^2 - 1) + \left( \frac{155}{693}x_1 + \frac{1}{693}x_2 + \frac{467}{3465}x_3 + \frac{34}{693}x_4 - \frac{842}{3465}x_1x_2x_3 \right. \\ & + \left. \frac{188}{693}x_1x_2x_4 - \frac{908}{3465}x_1x_3x_4 - \frac{292}{3465}x_2x_3x_4 \right) (x_1 + 3x_2 + 5x_3 + 2x_4). \end{aligned}$$

Note that the coefficient for  $(x_1^2 - 1)$  contains only even degree monomials that do not contain  $x_1$  (similarly for  $(x_2^2 - 1)$ , etc.) and that the coefficient for  $(x_1 + 3x_2 + 5x_3 + 2x_4)$  contains every possible odd degree monomial in four variables. The combinatorial interpretation of a number such as  $34/693$  is explicitly demonstrated in Ex. 9.  $\square$

### 3. The Partition Matrix: Definition and Properties

In this section, we explore the well-known connection between Hilbert's Nullstellensatz and linear algebra, in terms of the minimum-degree certificate defined in Thm. 2:

$$1 = \sum_{i=1}^n \left( \sum_{\substack{k \text{ even} \\ k \leq n-1}} \sum_{S \in S_k^{n \setminus i}} c_{i,S} x^S \right) (x_i^2 - 1) + \left( \sum_{\substack{k \text{ odd} \\ k \leq n}} \sum_{S \in S_k^n} b_S x^S \right) \left( \sum_{i=1}^n w_i x_i \right).$$

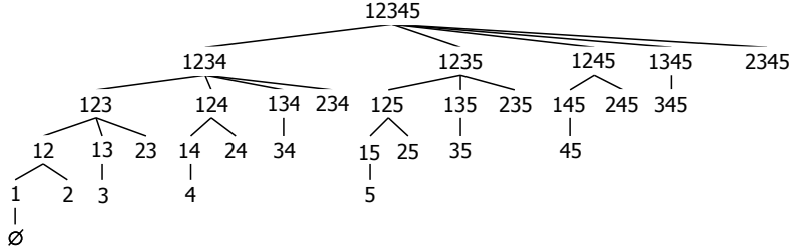
We begin by defining *graded reverse lexicographic order*. We then construct a  $2^{n-1} \times 2^{n-1}$  square system of linear equations containing only the unknowns  $b$ . When ordered according to *graded reverse lexicographic order*, this square matrix is known as the *partition matrix*. We conclude by demonstrating that the partition matrix is not only symmetric, but also has a variety of properties essential to proving our main result in Section 4.

#### 3.1. Graded Reverse Lexicographic Order as a Tree

Since we are dealing only with square-free monomials, we define *graded reverse lexicographic order* (denoted  $\succeq_D$ ) as follows. Given  $S \in S_k^n$ , we represent  $S$  as a vector in  $\{0, 1\}^n$  (denoted  $v_S$ ) by setting  $v_S[i] = 1$  if  $i \in S$  and  $v_S[i] = 0$  otherwise. For example, let  $S = \{2, 3, 7\} \in S_3^7$ . Then  $v_S = \{0, 1, 1, 0, 0, 0, 1\}$ . Given distinct  $S \in S_k^n$  and  $S' \in S_{k'}^n$ , then  $S \succeq_D S'$  in two cases: 1) if  $k > k'$ , or 2) if  $k = k'$  and the *right-most nonzero entry* of  $v_S - v_{S'}$  is negative. For example,  $\{2, 3, 4, 5\} \succeq_D \{1, 2, 5\}$ , and  $\{2, 3\} \succeq_D \{1, 4\}$ .

In order to prove specific properties of the partition matrix, we use a slightly less common, recursive definition of graded reverse lexicographic order. First, we order the  $\binom{n}{n-1}$  subsets of  $[n]$  in lexicographic order, creating sets  $S_1, \dots, S_n$ . Next, the sets  $S_1, \dots, S_n$  are iterated, and for each  $S_i$ , the  $\binom{n-1}{n-2}$  subsets of  $S_i$  are iterated in lexicographic order, etc.. This order is pictorially represented as a tree in Ex. 2.

**Example 2.** Here we pictorially order the set of integers  $[5]$  according to  $\succeq_D$ .



Using this tree, if two sets  $S, S'$  are from different levels in the tree with  $S$  higher than  $S'$ , then  $S \succeq_D S'$ . For example,  $\{1245\} \succeq_D \{234\}$ . Additionally, if  $S, S'$  are from the same level in the tree but  $S$  appears further to the left than  $S'$ , then  $S \succeq_D S'$ . For example,  $\{23\} \succeq_D \{15\}$ . Additionally, observe that if the even and odd cardinality subsets of  $[5]$  are iterated in  $\succeq_D$  order, then the following pairing of even and odd subsets occurs:

12345	123	124	134	234	125	135	235	145	245	345	1	2	3	4	5
1234	1235	1245	1345	2345	12	13	23	14	24	34	15	25	35	45	$\emptyset$

Given a set  $S$  in the pairing diagram above, if  $5 \in S$ , then  $S$  is paired with  $S \setminus 5$ . If  $5 \notin S$ , then  $S$  is paired with  $S \cup 5$ . This observation is proven in general in Prop. 3.3.  $\square$

We refer to this tree as the *order tree* of  $[n]$ . If two sets  $S, S'$  are children of the same parent in the tree, we say that the sets are contained in the same *block*. For example,  $\{1, 2, 3\}$  and  $\{2, 3, 4\}$  are in the same block, but  $\{2, 3, 4\}$  and  $\{1, 2, 5\}$  are not.

### 3.2. The Partition Matrix

In this section, we demonstrate how to extract a  $2^{n-1} \times 2^{n-1}$  matrix from the minimum-degree certificate of Thm. 2. We begin by considering the coefficients of  $(x_i^2 - 1)$ :

$$\left( \sum_{\substack{k \text{ even} \\ k \leq n-1}} \sum_{S \in S_k^{n \setminus i}} c_{i,S} x^S \right) (x_i^2 - 1) .$$

We observe that each monomial  $c_{i,S} x^S$  multiplies  $(x_i^2 - 1)$ , which implies that each  $c_{i,S}$  appears in two equations (one corresponding to the monomial  $x^S x_i^2$ , and one corresponding to the monomial  $-x^S$ ). Thus, the unknown  $c_{i,S}$  appears in the first equation with a positive coefficient, and the second equation with a negative coefficient. This allows us to sum the two equations, and cancel the  $c$  unknowns in a cascading manner. For example, there is always one equation for the constant term:

$$-c_{1,\emptyset} - c_{2,\emptyset} - \dots - c_{n,\emptyset} = 1 .$$

Notice that this equation sums to one, since the Nullstellensatz certificate simplifies to one. There is also always one equation for each  $x_i^2$  monomial:

$$b_i w_i + c_{i,\emptyset} = 0 . \tag{1}$$

The  $b_i w_i$  term appears in these equations since the product of

$$\left( \sum_{\substack{k \text{ odd} \\ k \leq n}} \sum_{S \in S_k^n} b_S x^S \right) (w_1 x_1 + \dots + w_n x_n) ,$$

contributes the term  $b_i x_i \cdot w_i x_i = b_i w_i x_i^2$ , among others. Notice that Eq. 1 sums to zero, since every monomial other than the constant term must cancel in a Nullstellensatz certificate. This set of  $n + 1$  equations yields the following subsystem:

$$\begin{aligned} -c_{1,\emptyset} - c_{2,\emptyset} - \dots - c_{n,\emptyset} &= 1 , & (\text{constant term}) \\ b_1 w_1 + c_{1,\emptyset} &= 0 , & (x_1^2) \\ &\vdots & \\ b_n w_n + c_{n,\emptyset} &= 0 . & (x_n^2) \end{aligned}$$

Summing these  $n + 1$  equations together yields the following equation (in  $b$  only):

$$\sum_{i=1}^n b_i w_i = 1 .$$

In general, let  $S \subseteq [n] \setminus i$  be an even cardinality subset, and consider the two monomials  $x^S x_i^2$  and  $x^S$ . Then, the following  $n - |S| + 1$  equations are always present in the extracted linear system:

$$\begin{aligned} b_{S \cup i} w_i + c_{i,S} &= 0 , & (x^S x_i^2) , & \text{for each } i \notin S \\ \sum_{j \in S} b_{S \setminus j} w_j - \sum_{i \notin S} c_{i,S} &= 0 , & (x^S) . \end{aligned} \tag{2}$$

Summing up these  $n - |S| + 1$  equations together yields the following equation (in  $b$  only):

$$\sum_{j \notin S} b_{S \cup j} w_j + \sum_{j \in S} b_{S \setminus j} w_j = 0 .$$

**Definition 1.** Given a set of integers  $W = \{w_1, \dots, w_n\}$ , the coefficient matrix of the following square system of linear equations

$$\begin{aligned} \sum_{j \notin S} b_{S \cup j} w_j + \sum_{j \in S} b_{S \setminus j} w_j &= 0 , \quad \text{for each } S \in (S_k^n \setminus \emptyset) \text{ with } |S| \text{ even} \\ \sum_{i=1}^n b_i w_i &= 1 , \end{aligned}$$

defines a  $2^{n-1} \times 2^{n-1}$  matrix with columns indexed by the unknowns  $b_S$  (corresponding to the  $2^{n-1}$  odd cardinality subsets of  $[n]$ ), and rows indexed by the sets  $S$  (corresponding to the  $2^{n-1}$  even cardinality subsets of  $[n]$ , including  $\emptyset$ ). This matrix is the partition matrix, denoted by  $\text{Part}_n$ , with rows and columns ordered by graded reverse lexicographic order.

By studying Eq. 2, we see that each  $c$  unknown appears in exactly one equation along with exactly one  $b$  unknown. Thus, solving for the  $b$  unknowns *uniquely determines the entire certificate*, and determining whether or not a given set  $W$  is partitionable depends entirely on the *determinant of the partition matrix*.

**Example 3.** Let  $W = \{w_1, w_2, w_3\}$ . Via Thm. 2, the Nullstellensatz certificate is:

$$\begin{aligned} 1 &= (c_{1,\emptyset} + c_{1,\{23\}} x_2 x_3)(x_1^2 - 1) + (c_{2,\emptyset} + c_{2,\{13\}} x_1 x_3)(x_2^2 - 1) + (c_{3,\emptyset} + c_{3,\{12\}} x_1 x_2)(x_3^2 - 1) \\ &\quad + (b_1 x_1 + b_2 x_2 + b_3 x_3 + b_{123} x_1 x_2 x_3)(w_1 x_1 + w_2 x_2 + w_3 x_3) . \end{aligned}$$

If  $W$  is not partitionable, there must exist an assignment to the unknowns  $c$  and  $b$  such that the certificate simplifies to one. In other words, the following system of linear equations has a solution:

$$\begin{array}{llll} \begin{pmatrix} x_1^2 \\ x_2^2 \\ x_3^2 \end{pmatrix} & \begin{matrix} c_{1,\emptyset} + b_1 w_1 = 0 , \\ c_{2,\emptyset} + b_2 w_2 = 0 , \\ c_{3,\emptyset} + b_3 w_3 = 0 , \end{matrix} & \begin{pmatrix} x_2 x_3 \\ x_1 x_2 x_3^2 \\ x_1 x_2^2 x_3 \end{pmatrix} & \begin{matrix} -c_{1,\{23\}} + b_2 w_3 + b_3 w_2 = 0 , \\ c_{3,\{12\}} + b_{123} w_3 = 0 , \\ c_{2,\{13\}} + b_{123} w_2 = 0 , \end{matrix} \\ \begin{pmatrix} x_1 x_2 \\ x_1 x_3 \end{pmatrix} & \begin{matrix} -c_{3,\{12\}} + b_1 w_2 + b_2 w_1 = 0 , \\ -c_{2,\{13\}} + b_1 w_3 + b_3 w_1 = 0 , \end{matrix} & \begin{pmatrix} x_1^2 x_2 x_3 \\ (constant \ term) \end{pmatrix} & \begin{matrix} c_{1,\{23\}} + b_{123} w_1 = 0 , \\ -c_{1,\emptyset} - c_{2,\emptyset} - c_{3,\emptyset} = 1 . \end{matrix} \end{array}$$

Following the simplifications described above, we extract a square system of linear equations that contain only the  $b$  unknowns from these equations:

$$\begin{aligned} b_{123} w_3 + b_1 w_2 + b_2 w_1 &= 0 , \quad S = \{1, 2\} , \quad b_{123} w_2 + b_1 w_3 + b_3 w_1 = 0 , \quad S = \{1, 3\} , \\ b_{123} w_1 + b_2 w_3 + b_3 w_2 &= 0 , \quad S = \{2, 3\} , \quad b_1 w_1 + b_2 w_2 + b_3 w_3 = 1 . \quad S = \emptyset . \end{aligned}$$

Ordering the columns as  $\{b_{123}, b_1, b_2, b_3\}$ , the partition matrix is as follows:

$$\begin{array}{cccc} & b_{123} & b_1 & b_2 & b_3 \\ \begin{matrix} \{1, 2\} \\ \{1, 3\} \\ \{2, 3\} \\ \emptyset \end{matrix} & \begin{bmatrix} w_3 & w_2 & w_1 & 0 \\ w_2 & w_3 & 0 & w_1 \\ w_1 & 0 & w_3 & w_2 \\ 0 & w_1 & w_2 & w_3 \end{bmatrix} \end{array}$$

As a preview of our main result, we note that the determinant of this matrix is

$$(w_1 + w_2 + w_3)(-w_1 + w_2 + w_3)(w_1 - w_2 + w_3)(-w_1 - w_2 + w_3) ,$$

which represents a brute-force iteration over all of the possible partitions of the set  $W$ . This will be formally defined as the partition polynomial in Sec. 4.  $\square$

For the duration of this section, we collect and prove a variety of interesting facts about the partition matrix  $\text{Part}_n$ . The properties may seem particularly intricate and overly specific, but each property is necessary in the proof the main result in Sec. 4. Throughout these propositions, the notation  $\text{Part}_n[i, :]$  follows standard MATLAB notation, and denotes the  $i$ -th row, whereas  $\text{Part}_n[i, 1 : j]$  denotes the  $i$ -th row with columns 1 through  $j$  only.

**Example 4.** Here we display the  $16 \times 16$  partition matrix  $\text{Part}_5$ .

	12345	123	124	134	234	125	135	235	145	245	345	1	2	3	4	5
1234	$w_5$	$w_4$	$w_3$	$w_2$	$w_1$	0	0	0	0	0	0	0	0	0	0	0
1235	$w_4$	$w_5$	0	0	0	$w_3$	$w_2$	$w_1$	0	0	0	0	0	0	0	0
1245	$w_3$	0	$w_5$	0	0	$w_4$	0	0	$w_2$	$w_1$	0	0	0	0	0	0
1345	$w_2$	0	0	$w_5$	0	0	$w_4$	0	$w_3$	0	$w_1$	0	0	0	0	0
2345	$w_1$	0	0	0	$w_5$	0	0	$w_4$	0	$w_3$	$w_2$	0	0	0	0	0
12	0	$w_3$	$w_4$	0	0	$w_5$	0	0	0	0	0	$w_2$	$w_1$	0	0	0
13	0	$w_2$	0	$w_4$	0	0	$w_5$	0	0	0	0	$w_3$	0	$w_1$	0	0
23	0	$w_1$	0	0	$w_4$	0	0	$w_5$	0	0	0	0	$w_3$	$w_2$	0	0
14	0	0	$w_2$	$w_3$	0	0	0	0	$w_5$	0	0	$w_4$	0	0	$w_1$	0
24	0	0	$w_1$	0	$w_3$	0	0	0	0	$w_5$	0	0	$w_4$	0	$w_2$	0
34	0	0	0	$w_1$	$w_2$	0	0	0	0	0	$w_5$	0	0	$w_4$	$w_3$	0
15	0	0	0	0	0	$w_2$	$w_3$	0	$w_4$	0	0	$w_5$	0	0	0	$w_1$
25	0	0	0	0	0	$w_1$	0	$w_3$	0	$w_4$	0	0	$w_5$	0	0	$w_2$
35	0	0	0	0	0	0	$w_1$	$w_2$	0	0	$w_4$	0	0	$w_5$	0	$w_3$
45	0	0	0	0	0	0	0	0	$w_1$	$w_2$	$w_3$	0	0	0	$w_5$	$w_4$
$\emptyset$	0	0	0	0	0	0	0	0	0	0	0	$w_1$	$w_2$	$w_3$	$w_4$	$w_5$

**Proposition 3.** The  $2^{n-1} \times 2^{n-1}$  matrix  $\text{Part}_n$  has the following properties:  $\square$

- (1) The entry  $w_i$  with  $i = \{1, \dots, n\}$  appears exactly once in each row and column.
- (2) The submatrix  $\text{Part}_n[1 : n, 1 : n]$  consists of  $w_n$  on the diagonal, the entries  $w_n, \dots, w_1$  in both  $\text{Part}_n[1 : n, 1]$  and  $\text{Part}_n[1, 1 : n]$ , and zero elsewhere.
- (3) If row  $i$  is indexed by set  $S \subseteq [n]$  (with  $|S|$  even), and  $n \in S$ , then column  $i$  is indexed by  $S \setminus n$ . If  $n \notin S$ , then column  $i$  is indexed by  $S \cup n$ .
- (4) All diagonal entries of  $\text{Part}_n$  are equal to  $w_n$ .
- (5) Given any row (column), the entries to the left (above) the diagonal are indexed by  $S \cup j$ , and the entries to the right (below) the diagonal are indexed by  $S \setminus j$ .
- (6)  $\text{Part}_n$  is symmetric.

*Proof of Prop. 3.1:* After inspecting the equation defining the partition matrix

$$\sum_{j \notin S} b_{S \cup j} w_j + \sum_{j \in S} b_{S \setminus j} w_j = 0 ,$$

where  $S$  represents an even cardinality subset of  $[n]$ , it is evident that each row contains



exactly one entry for each  $w_i$ . To see that each column also contains exactly one entry  $w_i$  with  $i = \{1, \dots, n\}$ , consider the column indexed by unknown  $b_{S'}$ , where  $S' \subseteq [n]$  with odd cardinality. Then, for each  $j \in S'$ , the row indexed by  $S = S' \setminus j$  contains  $w_j$ . Additionally, for each  $j \notin S'$ , the row indexed by  $S = S' \cup j$  also contains  $w_j$ . Thus, each row and column contains exactly one entry  $w_i$  for  $i = \{1, \dots, n\}$ .  $\square$

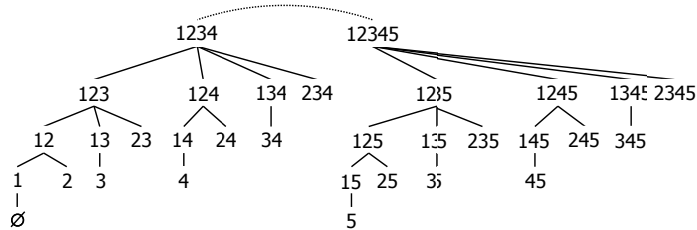
*Proof of Prop. 3.2:* We will prove that  $\text{Part}_n[1 : n, 1 : n]$  has the following form:

$$\begin{bmatrix} w_n & w_{n-1} & w_{n-2} & \cdots & w_1 \\ w_{n-1} & w_n & 0 & \cdots & 0 \\ w_{n-2} & 0 & w_n & 0 & \vdots \\ \vdots & \vdots & \ddots & \ddots & 0 \\ w_1 & 0 & \cdots & 0 & w_n \end{bmatrix}$$

For  $n$  even, row 1 is indexed by  $\{1 \cdots n\}$  and the first  $n$  columns are indexed by the  $\binom{n}{n-1}$  subsets of  $[n]$  in lexicographic order. Moreover, rows 2 through  $n$  are indexed by the  $\binom{n-1}{n-2}$  subsets of  $\{1 \cdots (n-1)\}$ . Therefore, the claim holds by inspecting the equation defining the partition matrix (Def. 1). For  $n$  odd, column 1 is indexed by  $\{1 \cdots n\}$  and the first  $n$  rows are similarly labeled with the  $\binom{n}{n-1}$  subsets of  $[n]$ . Moreover, columns 2 through  $n$  are indexed by the  $\binom{n-1}{n-2}$  subsets of  $\{1 \cdots (n-1)\}$ .  $\square$

As an example of Prop. 3.3, note that row  $\{12\}$  is paired with column  $\{125\}$ , and column  $\{1\}$  is paired with row  $\{15\}$  in Ex. 4.

*Proof of Prop. 3.3:* To prove this claim, suppose that we have the “order tree”  $T_{n-1}$  for the subsets of  $[n-1]$ . In order to create the order tree  $T_n$  for the subsets of  $[n]$ , we first copy  $T_{n-1}$  and add the integer  $n$  to each set, creating the tree  $T_{n-1} \cup n$ . We then join the node in  $T_{n-1} \cup n$  indexed by  $\{1 \cdots n\}$  to the node in  $T_{n-1}$  indexed  $\{1 \cdots (n-1)\}$ . The resulting tree is the order tree for  $T_n$ . For example,



Since no set in  $T_{n-1}$  contains the integer  $n$  and every set in  $T_{n-1} \cup n$  contains  $n$ , it is easy to see that the even and odd sets are paired by inspecting how  $T_{n-1}$  overlays on top of  $T_{n-1} \cup n$ . Thus, the claim holds.  $\square$

*Proof of Prop. 3.4:* This result follows from the equations defining the partition matrix, and also Prop. 3.3, which defines the row-column pairing of the diagonal element.  $\square$

*Proof of Prop. 3.5:* Consider a row indexed by the set  $S$ . Since  $S \cup j \succeq_D S \setminus j$ , we can be certain that the entries formed by  $S \cup j$  appear to the left (above) the entries formed by  $S \setminus j$ . The diagonal is either formed by  $S \cup n$  (if  $n \notin S$ ), or  $S \setminus n$  (if  $n \in S$ ). We observe that  $S \cup j \succeq_D S \cup n$  (if  $n \notin S$ ), and  $S \setminus n \succeq_D S$  (if  $n \in S$ ).  $\square$

*Proof of Prop. 3.6:* Consider an arbitrary row  $i$  indexed by a set  $S_i$ , and let column  $i$  be indexed by the set  $b_i$ . In order to prove symmetry, we must show that row  $i$  is equal to column  $i$ . By Prop. 3.3,  $n$  is either in  $S_i$  or  $b_i$ , but not both. Without loss of generality, assume  $n \in S_i$  and  $b_i = S_i \setminus n$  (e.g.  $S_i = \{15\}$  and  $b_i = \{1\}$ ). Suppose  $\text{Part}_n[i, j] = w_{k_j}$  for

$j < i$ . We must show that  $\text{Part}_n[j, i] = w_{k_j}$ . Since  $j < i$ ,  $k_j \notin S_i$ , and column  $j$  is indexed by  $b_j = S_i \cup k_j$  (e.g. in row  $\{15\}$ ,  $w_2$  appears in column  $\{125\}$ ). Since  $n \in (S_i \cup k_j)$ , row  $j$  is indexed by  $S_j = (S_i \cup k_j) \setminus n$  (e.g.  $S_j = \{12\}$ ). Then,  $S_j \setminus k_j = b_i$ , and  $\text{Part}_n[j, i] = w_{k_j}$ .

Suppose  $i < j$ , and  $\text{Part}_n[i, j]$  is again equal to  $w_{k_j}$ . Then  $k_j \in S_i$ , and column  $j$  is indexed by  $b_j = S_i \setminus k_j$  and row  $j$  is indexed by  $S_j = (S_i \setminus k_j) \setminus n$  (e.g., in row  $\{15\}$ ,  $w_1$  appears in column  $\{1\}$ ). But then  $S_j \cup k_j = b_i$ , and  $\text{Part}_n[j, i] = w_{k_j}$ .

A similar argument holds if  $n \notin S_i$ , but with the logic reversed. Since we have shown that  $\text{Part}_n[i, j] = \text{Part}_n[j, i]$ , we have shown that the matrix is symmetric.  $\square$

**Proposition 4.** *Let column  $j$  be indexed by set  $\{j_1 \cdots j_k\}$ , where  $j_1, \dots, j_r$  are consecutive ascending integers excluding  $n$ , and let column  $j + 1 \leq 2^{n-1}$  be indexed by set  $\{j'_1, \dots, j'_{k'}\}$  where  $j'_1, \dots, j'_{r'}$  are consecutive ascending integers.*

- (1) *If  $j_1 = 1$ , then  $\exists$  a row  $i$  such that  $\text{Part}_n[i : (i + r - 1), j] = \{w_r, \dots, w_1\}$ .*
- (2) *If  $j_1 = j'_1 = 1$ , then  $\exists$  a row  $i$  such that  $\text{Part}_n[(i + r) : (i + 2r - 2), j + 1] = \{w_{r-1}, \dots, w_1\}$ .*
- (3) *If  $j_1 \neq 1$ , then let  $1, \dots, t$  be the integers such that  $t = j_1 - 1$ . Then,  $\exists$  a row  $i'$  such that  $\text{Part}_n[i' : (j - t) : j] = \{w_1, \dots, w_{t+1}\}$ .*
- (4) *If  $j_1 \neq 1$  and  $j'_1 = 1$ , then, given the rows  $i$  and  $i'$  that exist by claims (1) and (3), respectively,  $i = i' + 1$ .*

Before proving claim 4.1, we study an example. In Ex. 4, column 1 is indexed by set  $\{12345\}$ , and thus contains a set of consecutive ascending integers (excluding  $n$ ) equal to  $\{1, 2, 3, 4\}$ . Notice that  $\text{Part}_5[2 : 5, 1] = \{w_4, w_3, w_2, w_1\}$ . Additionally, column 2 is indexed by set  $\{123\}$ , and thus has a consecutive ascending set of integers equal to  $\{1, 2, 3\}$ . Furthermore,  $\text{Part}_5[6 : 8, 2] = \{w_3, w_2, w_1\}$ . Thus, for column 1, the row  $i$  referred to in claim (1) is  $i = 2$ , and for column 2, the row  $i$  referred to in claim (1) is  $i = 6$ . Given a column  $j$ , we will refer to the entries in  $\text{Part}_n[i : (i + r - 1), j] = \{w_r, \dots, w_1\}$  as the “trailing block” of column  $j$ .

**Example 5.** *Here we highlight the trailing blocks of each applicable column.*

	123	124	134	234	1	2	3	4
1234	$w_4$	$w_3$	$w_2$	$w_1$	0	0	0	0
12	$\mathbf{w}_3$	$w_4$	0	0	$w_2$	$w_1$	0	0
13	$\mathbf{w}_2$	0	$w_4$	0	$w_3$	0	$w_1$	0
23	$\mathbf{w}_1$	0	0	$w_4$	0	$w_3$	$w_2$	0
14	0	$\mathbf{w}_2$	$w_3$	0	$w_4$	0	0	$w_1$
24	0	$\mathbf{w}_1$	0	$w_3$	0	$w_4$	0	$w_2$
34	0	0	$\mathbf{w}_1$	$w_2$	0	0	$w_4$	$w_3$
$\emptyset$	0	0	0	0	$\mathbf{w}_1$	$w_2$	$w_3$	$w_4$

*Proof of Prop. 4.1:* If the set  $\{j_1 \cdots j_k\}$  indexing column  $j$  has  $j_1 = 1$ , then the set of consecutive ascending integers  $\{j_1 \cdots j_r\}$  is  $\{1 \cdots r\}$ . Recall that odd order sets index the columns, and even order sets index the rows. Thus, the even order sets

$$\begin{aligned}
&\{1 \cdots r j_{r+1} \cdots j_k\} \setminus r, \\
&\{1 \cdots r j_{r+1} \cdots j_k\} \setminus (r - 1), \\
&\vdots \\
&\{1 \cdots r j_{r+1} \cdots j_k\} \setminus 1,
\end{aligned}$$

index the consecutive block of rows from some row  $i$  to row  $i + r - 1$ . By the definition

of the partition matrix  $\text{Part}_n$  (Def. 1), if column  $j$  is indexed by set

$$\{1 \cdots r j_{r+1} \cdots j_k\}$$

and row  $i$  is indexed by set

$$\{1 \cdots r j_{r+1} \cdots j_k\} \setminus r ,$$

then  $\text{Part}_n[i, j] = w_r$ , since  $r$  is contained in the column set, but *not* contained in the row set. Thus,  $\text{Part}_n[i : (i + r - 1), j] = \{w_r, \dots, w_1\}$  and the claim is proven.  $\square$

As an example of claim 4.2, we recall in Ex. 4, that column 1 is indexed by set  $\{12345\}$ , containing consecutive ascending integers (excluding  $n$ ) equal to  $\{1, 2, 3, 4\}$ . Therefore,  $r = 4$ , since there are *four* consecutive ascending integers. Recall further that column 2 is indexed by set  $\{123\}$ , containing a consecutive ascending set of integers  $\{1, 2, 3\}$ . Therefore,  $r' = 3$ , since there are *three* consecutive ascending integers within the label. Observe that the size of the consecutive ascending set of integers in column 2 is *one less* than the size of the consecutive ascending set of integers in column 1 (excluding  $n$ ). We claim in Prop. 4.2 that  $\text{Part}_n[(i + r) : (i + 2r - 2), j + 1] = \{w_{r-1}, \dots, w_1\}$ , and we observe that  $\text{Part}_5[(2 + 4) : (2 + 2 \cdot 4 - 2), 1 + 1] = \text{Part}_5[6 : 8, 2] = \{w_3, w_2, w_1\}$ . Thus, claim (4.2) holds in this example.

*Proof of Prop. 4.2:* By Prop. 3.1,  $\text{Part}_n[i : (i + r - 1), j] = \{w_r, \dots, w_1\}$ . Assume that  $k = k'$ . In this case, since the set indexing column  $j$  and the set indexing column  $(j + 1)$  both contain 1, both sets are contained within the same block (have the same parent within the order tree). Therefore, by the lexicographic ordering present within a given block, column  $j$  is indexed by  $\{1 \cdots r j_{r+1} \cdots j_k\}$  and column  $j + 1$  is indexed by  $\{j'_1 \cdots j'_{r'} j'_{r'+1} \cdots j'_{k'}\} = \{1 \cdots (r - 1)(r + 1) j'_{r+1} \cdots j'_{k'}\} = \{1 \cdots (r - 1)(r + 1) j_{r+1} \cdots j_k\}$ . For example, suppose column  $j$  is indexed  $\{1236789\}$ . Then column  $j + 1$  must be indexed by  $\{1246789\}$  according to lexicographic order. In other words,  $r' = r - 1$ ,  $j'_{r'+1} = r + 1$  and  $j'_{r'+2} = j_{r+1}$ . Therefore, the even order sets

$$\begin{aligned} & \{1 \cdots (r - 1)(r + 1) j_{r+1} \cdots j_k\} \setminus (r - 1) , \\ & \{1 \cdots (r - 1)(r + 1) j_{r+1} \cdots j_k\} \setminus (r - 2) , \\ & \vdots \\ & \{1 \cdots (r - 1)(r + 1) j_{r+1} \cdots j_k\} \setminus 1 , \end{aligned}$$

index the consecutive block of rows from row  $i + r$  to row  $i + r + (r - 1) - 1$ . Therefore, by the definition of the partition matrix (Def. 1),  $\text{Part}_n[(i + r) : (i + 2r - 2), j] = \{w_{r-1}, \dots, w_1\}$  and the claim is proven.

If  $k' \neq k$  and  $j_1 = j'_1 = 1$ , then this is the special case that only occurs in column 1 and column 2 when  $n$  is odd. In this case, column 1 is indexed by  $\{1 \cdots n\}$ , and column 2 is indexed by  $\{1 \cdots (n - 2)\}$ . Additionally, the first  $n$  rows are indexed by the  $\binom{n}{n-1}$  subsets, and the next  $n - 1$  rows are indexed by the  $\binom{n-1}{n-2}$  subsets of  $[n - 1]$ . Therefore,  $\text{Part}_n[2 : n, 1] = \{w_{n-1}, \dots, w_1\}$  and  $\text{Part}_n[(n + 1) : (2n - 2), 2] = \{w_{n-2}, \dots, w_1\}$  as claimed. In either case, the claim holds.  $\square$

As an example of Prop. 4.3, we observe that in Ex. 4, row  $\{45\}$  contains entries  $\{w_1, w_2, w_3\}$  in the columns indexed  $\{145\}, \{245\}, \{345\}$ , respectively.

*Proof of Prop. 4.3:* Since column  $j$  is indexed by  $\{j_1 \cdots j_k\}$  and  $j_1 \neq 1$ , this means that the last row of column  $j$  containing an entry is the row indexed by the set  $\{j_1 \cdots j_k\} \setminus j_1 =$

$\{j_2 \cdots j_k\}$ . Furthermore, the columns indexed by

$$\begin{aligned} & \{(j_1 - 1)j_2 \cdots j_k\}, \\ & \{(j_1 - 2)j_2 \cdots j_k\}, \\ & \vdots \\ & \{1j_2 \cdots j_k\}, \end{aligned}$$

are the columns  $j-1, j-2, \dots, j-j_1+1$ , respectively. Thus, the row indexed by  $\{j_2 \cdots j_k\}$  contains entries  $w_1, \dots, w_{j_1}$  in columns  $j-j_1+1, \dots, j-1, j$ , respectively, and the claim is proved.  $\square$

In order to clarify the statement of the Prop. 4.4, we observe that in Ex. 4, the column labeled with set  $\{345\}$  has the row indexed by set  $\{45\}$  ( $i' = 15$ ), and the next column (indexed by  $\{1\}$ ) has the row indexed  $\{\emptyset\}$  ( $i = 16$ ). Therefore,  $i = i' + 1$  and  $|\{345\}| - |\{1\}| = 3 - 1 = 2$ , and the condition holds.

*Proof of Prop. 4.4:* In this claim,  $j_1 \neq 1$  and  $j'_1 = 1$ . We begin by assuming that  $k' = k-2$ . In this case, column  $j$  and column  $j+1$  are indexed by sets from two different levels of the order tree. Furthermore, since  $j$  is indexed by the set at the *end* of a level,  $n = j_k$ , and  $\{j_1 \cdots j_k\}$  is actually equal to  $\{(n-k+1) \cdots n\}$ . This implies that the row  $i'$  from claim 3 is indexed by  $\{j_1 \cdots j_k\} \setminus j_1$ , or  $\{(n-k+1) \cdots n\} \setminus (n-k+1)$ . Since the set labeling column  $j+1$  is the *first* set in the next odd level,  $\{j'_1 \cdots j'_{k'}\} = \{1 \cdots k'\}$ . Therefore, the row  $i$  from claim 1 is  $\{1 \cdots k'\} \setminus k' = \{1 \cdots (k-2)\} \setminus (k-2)$ . But clearly  $\{1 \cdots (k-2)\} \setminus (k-2)$  labels the row directly *after*  $\{(n-k+1) \cdots n\} \setminus (n-k+1)$ . Therefore,  $i = i' + 1$  as claimed.

In the second case, we assume  $k' = k$ . Thus, the two sets labeling columns  $j$  and  $j+1$  respectively are in the *same* level of the order tree. However, since  $j_1 \neq 1$  and  $j'_1 = 1$ , the two sets are from different blocks in the same level. Moreover, the set labeling column  $j$  is at the end of one block, and the set labeling column  $j+1$  is at the beginning of the next block. Therefore, the set labeling  $j$  is  $\{j_1 \cdots j_r j_{r+1} j_k\}$ , and the set labeling column  $j+1$  is  $\{1 \cdots (r-1)(j_r+1)j_{r+1} \cdots j_k\}$ . Thus, we see that the row  $i'$  from 4.3 associated with column  $j$  is indexed by  $\{j_1 \cdots j_r j_{r+1} j_k\} \setminus j_1$ . The row  $i$  from 4.1 associated with column  $j+1$  is indexed by  $\{1 \cdots (r-1)(j_r+1)j_{r+1} \cdots j_k\} \setminus (r-1)$ . These two rows,

$$\begin{aligned} & \{j_1 \cdots j_r j_{r+1} j_k\} \setminus j_1, \quad \text{and} \\ & \{1 \cdots (r-1)(j_r+1)j_{r+1} \cdots j_k\} \setminus (r-1) \end{aligned}$$

are lexicographically adjacent. Therefore,  $i = i' + 1$  as claimed.

Since the claim holds in both cases, 4.4 is proved.  $\square$

The following three propositions deal with identifying similar blocks of entries in different rows and columns. Within these propositions, we will use the following notation. Given a column  $j$ , let  $A_j$  denote the set of entries *above* the diagonal. Notice that the set  $A_j \subseteq \{w_1, \dots, w_{n-1}\}$  since  $w_n$  is never in  $A_j$  because  $w_n$  is always on the diagonal.

**Proposition 5.** *Let  $j$  be a column indexed by  $\{1j_2 \cdots j_k\}$ . Let  $i$  be any row in the trailing block of column  $j$ . Then, the non-zero entries in  $\text{Part}_n[i, (j+1) : (i-1)]$  are the same as the entries in  $A_j$ .*

**Example 6.** Here is an example of Prop 5. Let  $j$  be column  $\{124\}$ . Then the trailing block of column  $j$  consists of entries  $\{w_2, w_1\}$ , and  $A_j = \{w_3\}$ . Let  $i$  be either row in the trailing block, either  $\{14\}$  or  $\{24\}$ . Then the only non-zero entry in  $\text{Part}_n[i, (j+1) : (i-1)]$  is  $\{w_3\}$ , which is exactly equal to  $A_j$ .

	123	124	134	234	1	2	3	4
1234	$w_4$	<b><math>w_3</math></b>	$w_2$	$w_1$	0	0	0	0
12	$w_3$	$w_4$	0	0	$w_2$	$w_1$	0	0
13	$w_2$	0	$w_4$	0	$w_3$	0	$w_1$	0
23	$w_1$	0	0	$w_4$	0	$w_3$	$w_2$	0
14	0	$w_2$	<b><math>w_3</math></b>	0	$w_4$	0	0	$w_1$
24	0	$w_1$	0	<b><math>w_3</math></b>	0	$w_4$	0	$w_2$
34	0	0	$w_1$	$w_2$	0	0	$w_4$	$w_3$
$\emptyset$	0	0	0	0	$w_1$	$w_2$	$w_3$	$w_4$

□

*Proof of Prop. 5:* Given a column  $j$  indexed by  $\{1j_2 \cdots j_k\}$ , let  $i$  be a row in the trailing block of column  $j$  such that  $P[i, j] = w_t$ . Then row  $i$  is indexed by set  $\{1j_2 \cdots j_k\} \setminus t$ . We will show that the set of non-zero entries in  $\text{Part}_n[i, (j+1) : (i-1)]$  are the *same* as the set of entries above the diagonal in column  $j$ , denoted by  $A_j$ .

We will prove both directions of the inclusion. First, we will prove that  $A_j \subseteq \text{Part}_n[i, (j+1) : (i-1)]$ . Let  $w_a \in A_j$ . Then  $a \notin \{1j_2 \cdots j_k\}$ . Moreover, the column indexed by  $\{\{1j_2 \cdots j_k\} \setminus t\} \cup a$  falls *between* columns  $j$  and the diagonal. Therefore, the entry  $\text{Part}_n[i, i'] = w_a$  where  $j+1 \leq i' \leq i-1$ .

Conversely, let  $\text{Part}_n[i, i'] = w_a$  where  $j+1 \leq i' \leq i-1$ . Then,  $a \notin \{1j_2 \cdots j_k\}$ , which implies  $w_a \in A_j$ .

Since we have proven both directions, the non-zero entries in  $\text{Part}_n[i, (j+1) : (i-1)]$  are the *same* as the set  $A_j$ . □

**Proposition 6.** Let  $j$  be a column indexed by  $\{1j_2 \cdots j_k\}$ . Let  $i$  be any row in the trailing block of column  $j$ . Let  $j < i' < i$  be such that  $P[i, i']$  is non-zero. Then  $A_j \cup P[i, j] = A_{i'} \cup P[i, i']$ .

**Example 7.** Here is an example of Prop 6. Let  $j$  be column  $\{124\}$ . Then the trailing block of column  $j$  consists of entries  $\{w_2, w_1\}$ , and  $A_j = \{w_3\}$ . Let  $i$  be row  $\{14\}$  in the trailing block, and let  $i'$  be column  $\{234\}$ . Then  $A_j \cup P[i, j] = \{w_3\} \cup \{w_1\} = \{w_1\} \cup \{w_3\} = A_{i'} \cup P[i, i']$ .

	123	124	134	234	1	2	3	4
1234	$w_4$	<b><math>w_3</math></b>	$w_2$	<b><math>w_1</math></b>	0	0	0	0
12	$w_3$	$w_4$	0	0	$w_2$	$w_1$	0	0
13	$w_2$	0	$w_4$	0	$w_3$	0	$w_1$	0
23	$w_1$	0	0	$w_4$	0	$w_3$	$w_2$	0
14	0	$w_2$	$w_3$	0	$w_4$	0	0	$w_1$
24	0	<b><math>w_1</math></b>	0	<b><math>w_3</math></b>	0	$w_4$	0	$w_2$
34	0	0	$w_1$	$w_2$	0	0	$w_4$	$w_3$
$\emptyset$	0	0	0	0	$w_1$	$w_2$	$w_3$	$w_4$

□

*Proof of Prop. 6:* Let column  $j$  be indexed by  $\{1j_2 \cdots j_k\}$ , and let  $i$  be a row in the trailing block of column  $j$  such that  $P[i, j] = w_t$ . Then, row  $i$  is indexed by set  $\{1j_2 \cdots j_k\} \setminus t$ . If row  $i$  contains a non-zero entry  $P[i, i'] = w_a$  before the diagonal, then column  $i'$  is indexed by  $\{\{1j_2 \cdots j_k\} \setminus t\} \cup a$ . Since  $a$  is not in  $\{1j_2 \cdots j_k\}$ , then  $a$  is in  $A_j$ . Moreover, since  $t$  is not in the set labeling the column  $i'$ , then  $t \in A_{i'}$ . Since every other index between the two column labels ( $\{1j_2 \cdots j_k\}$  and  $\{\{1j_2 \cdots j_k\} \setminus t\} \cup a$ ) is the same,  $A_j \cup w_t = A_{i'} \cup w_a$ , or  $A_j \cup P[i, j] = A_{i'} \cup P[i, i']$ . □

**Proposition 7.** *Let  $j$  be a column indexed by  $\{1j_2 \cdots j_k\}$ . Let  $i$  be any row in the trailing block of column  $j$ . Let  $i < i'$ . Then  $A_j \cup P[i, j] \cup P[i, i'] = A_{i'}$ .*

**Example 8.** *Here is an example of Prop 7. Let  $j$  be column  $\{124\}$ . Then the trailing block of column  $j$  consists of entries  $\{w_2, w_1\}$ , and  $A_j = \{w_3\}$ . Let  $i$  be row  $\{24\}$  in the trailing block, and let  $i'$  be column  $\{4\}$ . Then,  $A_j \cup P[i, j] \cup P[i, i'] = \{w_3\} \cup \{w_1\} \cup \{w_2\} = \{w_1, w_2, w_3\} = A_{i'}$ .*

	123	124	134	234	1	2	3	4
1234	$w_4$	<b><math>w_3</math></b>	$w_2$	$w_1$	0	0	0	0
12	$w_3$	$w_4$	0	0	$w_2$	$w_1$	0	0
13	$w_2$	0	$w_4$	0	$w_3$	0	$w_1$	0
23	$w_1$	0	0	$w_4$	0	$w_3$	$w_2$	0
14	0	$w_2$	$w_3$	0	$w_4$	0	0	<b><math>w_1</math></b>
24	0	<b><math>w_1</math></b>	0	$w_3$	0	$w_4$	0	<b><math>w_2</math></b>
34	0	0	$w_1$	$w_2$	0	0	$w_4$	<b><math>w_3</math></b>
∅	0	0	0	0	$w_1$	$w_2$	$w_3$	$w_4$

□

*Proof of Prop. 7:* Let column  $j$  be indexed by  $\{1j_2 \cdots j_k\}$ , and let  $i$  be a row in the trailing block of column  $j$  such that  $P[i, j] = w_t$ . Then, row  $i$  is indexed by set  $\{1j_2 \cdots j_k\} \setminus t$ . If row  $i$  contains a non-empty entry  $P[i, i'] = w_a$  after the diagonal, then column  $i'$  is indexed by  $\{\{1j_2 \cdots j_k\} \setminus t\} \cup a$ . Since  $a$  is in  $\{1j_2 \cdots j_k\}$ , then  $a$  is not in  $A_j$ , but it is in  $A_{i'}$  (since it is above the diagonal in column  $i'$ ). Moreover, since  $t$  is not in the set labeling column  $i'$ , then  $t \in A_{i'}$ . Since every other index between the two column labels ( $\{1j_2 \cdots j_k\}$  and  $\{\{1j_2 \cdots j_k\} \setminus t\} \cup a$ ) is the same,  $A_j \cup w_t \cup w_a = A_{i'}$ , or  $A_j \cup P[i, j] \cup P[i, i'] = A_{i'}$ . □

Having gathered together a series of facts about the partition matrix, we will now investigate the determinant of the partition matrix.

## 4. The Partition Matrix and Partition Polynomial

Given a square non-singular matrix  $A$ , Cramer's rule states that  $Ax = b$  can be solved by

$$x_i = \frac{\det(A|_b^i)}{\det(A)},$$

where  $A|_b^i$  is the matrix  $A$  with the  $i$ -th column replaced with the right-hand side vector  $b$ . In Section 3, we extracted a  $2^{n-1} \times 2^{n-1}$  square linear system from the general linear

system constructed via the minimum-degree Nullstellensatz certificate described by Thm. 2. Here, we see by Cramer's rule that the unknowns within that certificate are ratios of two determinants. In this section, we show that the determinant of the partition matrix is equivalent to a brute-force iteration over all the partitions of  $W$ . Therefore, the denominator of any unknown in the certificate is a combinatorial representation of the partition problem.

We observe that, in general, the linear system  $Ax = b$  may have a solution even if  $\det(A) = 0$ . However, in the case of the partition matrix, when we demonstrate that the  $\det(A)$  is equal to the *partition polynomial*, we will be demonstrating that  $Ax = b$  only has a solution in the case when  $\det(A) \neq 0$ .

Let  $\{0, 1\}^n$  be the set of all 0/1 bit strings of length  $n$ . For  $S \in \{0, 1\}^n$ , let  $S_i$  denote the  $i$ -th bit in the string  $S$ .

**Definition 2.** Given a set  $W = \{w_1, \dots, w_n\}$ , let

$$\prod_{S \in \{0, 1\}^{n-1}} \left( \left( \sum_{i=1}^{n-1} (-1)^{S_i} w_i \right) + w_n \right)$$

be the partition polynomial of  $W$ .

For example, let  $n = 5$ , and  $S \in \{0, 1\}^4$  be  $S = "1011"$ . Then,  $S$  corresponds to the  $-w_1 + w_2 - w_3 - w_4$ , and denotes a partition of  $W = \{w_1, \dots, w_5\}$ , with  $w_5$  fixed on the "positive" side of the partition, and the other  $w_i$  sorted according to sign.

$$\begin{array}{c|c} - & + \\ \hline w_1 & w_5 \\ w_3 & w_2 \\ w_4 & \end{array}$$

If this arrangement of  $w_i$  is a partition of  $W$ , then  $-w_1 + w_2 - w_3 - w_4 + w_5 = 0$ . In this way, *any* bitstring  $S \in \{0, 1\}^{n-1}$  is equivalent to fixing  $w_n$  on the "positive" side of the partition, and then arranging the other  $w_i$  on the "positive/negative" side, according to sign. In this way, the partition polynomial represents an iteration over *every possible partition* of  $W$ , avoiding double-counting by permanently fixing  $w_n$  on the "positive" side. If the set  $W$  is partitionable, one of bitstrings  $S$  will define a factor of the partition polynomial that sums to zero. We will show that the determinant of the partition matrix is the partition polynomial: therefore, if the determinant of the partition matrix is zero, the linear system has *no* solution, and there is *no* Nullstellensatz certificate.

**Example 9.** In Ex. 1, we presented an actual minimum-degree certificate for the non-partitionable set  $W = \{1, 3, 5, 2\}$ . We observe that

$$\begin{aligned} -51975 &= (1 + 3 + 5 + 2)(-1 + 3 + 5 + 2)(1 - 3 + 5 + 2)(1 + 3 - 5 + 2) \\ &\quad (-1 - 3 + 5 + 2)(-1 + 3 - 5 + 2)(1 - 3 - 5 + 2)(-1 - 3 - 5 + 2) . \end{aligned}$$

Via Cramer's rule, we see that the unknown  $b_4$  is equal to

$$b_4 = \frac{-2550}{-51975} = \frac{34}{693} ,$$

which is indeed the value of unknown  $b_4$  as it appears in the certificate.  $\square$

**Example 10.** Here is the determinant of the  $8 \times 8$  partition matrix  $Part_4$ :

$$\det \begin{pmatrix} w_4 & w_3 & w_2 & w_1 & 0 & 0 & 0 & 0 \\ w_3 & w_4 & 0 & 0 & w_2 & w_1 & 0 & 0 \\ w_2 & 0 & w_4 & 0 & w_3 & 0 & w_1 & 0 \\ w_1 & 0 & 0 & w_4 & 0 & w_3 & w_2 & 0 \\ 0 & w_2 & w_3 & 0 & w_4 & 0 & 0 & w_1 \\ 0 & w_1 & 0 & w_3 & 0 & w_4 & 0 & w_2 \\ 0 & 0 & w_1 & w_2 & 0 & 0 & w_4 & w_3 \\ 0 & 0 & 0 & 0 & w_1 & w_2 & w_3 & w_4 \end{pmatrix} = \begin{pmatrix} (w_1 + w_2 + w_3 + w_4)(-w_1 + w_2 + w_3 + w_4) \\ (w_1 - w_2 + w_3 + w_4)(w_1 + w_2 - w_3 + w_4) \\ (-w_1 + w_2 - w_3 + w_4)(-w_1 - w_2 + w_3 + w_4) \\ (w_1 - w_2 - w_3 + w_4)(-w_1 - w_2 - w_3 + w_4) \end{pmatrix}.$$

**Theorem 8.** Given  $W = \{w_1, \dots, w_n\}$ , the determinant of the partition matrix of  $W$  is the partition polynomial of  $W$ .

We will prove this theorem in a slightly unconventional way. Recall that

$$\det(A) = \sum_{\sigma \in S_n} \text{sgn}(\sigma) \prod_{i=1}^n A_{i, \sigma_i}.$$

for an  $n \times n$  matrix  $A$ . Via this formula, we can see that the determinant of the partition matrix is a degree  $2^{n-1}$  polynomial. Therefore, if we can show that each of the  $2^{n-1}$  factors of the partition polynomial are also factors of the determinant of the partition matrix, we will have provided a unique factorization for the determinant, and thus illustrated that the determinant of the partition matrix is equal to the partition polynomial.

Given  $S \in \{0, 1\}^{n-1}$ , if we make the substitution

$$w_n = - \left( \sum_{i=1}^{n-1} (-1)^{S_i} w_i \right)$$

into the partition matrix, and then demonstrate that the determinant of the partition matrix *after* the substitution is zero, we will have shown that the factor defined by the bitstring  $S$  is a root of the determinant. If we can prove this claim for *any* bitstring  $S \in \{0, 1\}^{n-1}$ , we will have proven Thm. 8. Consider the following algorithm:

```
*****
ALGORITHM: FACTORCHECK
  INPUT: An integer  $n$  and a factor  $S \in \{0, 1\}^{n-1}$ .
  OUTPUT: The reduced  $2^{n-1} \times 2^{n-1}$  matrix  $P$  with factor  $S$  substituted for  $w_n$ .
1  Set  $P = \text{Part}_n$  (Def. 1), set  $w_n = - \left( \sum_{i=1}^{n-1} (-1)^{S_i} w_i \right)$  in  $P$ , and set  $i = 2$ .
4  for  $j = 1$  to  $2^{n-1}$  do
5    while  $P(1, j) \neq 0$  do
6      Set  $w_t = P[i, j]$ , and set  $cur\_sgn = -(\text{sign of } w_t \text{ in cell } P(1, j))$ .
8      Set  $P(1, :) = cur\_sgn \cdot P(i, :) + P(1, :)$ .
9      Set  $i = i + 1$ .
10   end while
11 end for
12 return  $P$ .
*****
```



For example, suppose  $P[1, j] = w_1 + w_2 - w_3$ , and  $P[i : (i + 2), j] = \{w_3, w_2, w_1\}$ . Then, after applying the following row operations

$$\begin{aligned} P[1, :] &= P[i, :] + P[1, :] , \\ P[1, :] &= -P[i + 1, :] + P[1, :] , \\ P[1, :] &= -P[i + 2, :] + P[1, :] , \end{aligned}$$

the entry  $P[1, j] = 0$ .

In Appendix A, we demonstrate an example of the algorithm running step-by-step on a particular integer  $n$  and input factor  $S$ . We will show that when this algorithm terminates, the first row of the output matrix  $P$  consists entirely of zeros. This would demonstrate that the factor described by the particular input bitstring  $S$  is a root of the determinant. Since we will show the result holds for *any* bitstring  $S$ , this will have shown that the determinant is the partition polynomial, and conclude the proof of Thm 8.

When proving that an algorithm is “correct” (i.e., has the desired outcome), the technique is to define a loop invariant, and then show *initialization*, *maintenance* and *termination*:

- **Initialization:** The invariant is true prior to the first iteration of the loop.
- **Maintenance:** If the invariant is true before the current iteration of the loop, then the invariant is true before the next iteration of the loop.
- **Termination:** When the loop terminates, the loop invariant provides a useful property that helps show that the algorithm is correct.

Given a column  $j$  indexed by  $\{j_1 \cdots j_k\}$ , let  $T_j = \{j_1, \dots, j_r\} \subseteq [n - 1]$  be the longest sequence of consecutive ascending integers (excluding  $n$ ), or the *trailing block*, as in Prop. 4.1. Let  $A_j \subseteq [n - 1]$  be the set of entries above the diagonal in column  $j$ , and let  $B_j = [n - 1] \setminus (A_j \cup T_j)$  be the set of entries below the diagonal, excluding the trailing block.

**Example 11.** In column  $\{124\}$ , we highlight the trailing block  $T_{124}$ . In column  $\{134\}$ , we highlight the set  $B_{134}$ , and in column  $\{1\}$  we highlight the set  $A_1$ .

	123	124	134	234	1	2	3	4
1234	$w_4$	$w_3$	$w_2$	$w_1$	0	0	0	0
12	$w_3$	$w_4$	0	0	<b><math>w_2</math></b>	$w_1$	0	0
13	$w_2$	0	$w_4$	0	<b><math>w_3</math></b>	0	$w_1$	0
23	$w_1$	0	0	$w_4$	0	$w_3$	$w_2$	0
14	0	<b><math>w_2</math></b>	<b><math>w_3</math></b>	0	$w_4$	0	0	$w_1$
24	0	<b><math>w_1</math></b>	0	$w_3$	0	$w_4$	0	$w_2$
34	0	0	$w_1$	$w_2$	0	0	$w_4$	$w_3$
$\emptyset$	0	0	0	0	$w_1$	$w_2$	$w_3$	$w_4$

Finally, let

$$\begin{aligned} \text{sgn}(a, A_j) &= \prod_{e \in A_j \setminus a} (-1)^{S_e} , \text{ for each } a \in A_j , \\ \text{sgn}(A_j) &= \prod_{e \in A_j} (-1)^{S_e} . \end{aligned}$$

Note that  $\text{sgn}(a, A_j)$  and  $\text{sgn}(A_j)$  are both  $\pm 1$ . Since the FACTORCHECK algorithm contains the variables  $i, j, P$  and the input factor bitstring  $S$ , any loop invariant for the algorithm FACTORCHECK can be expressed in terms of those variables. We will also describe the conditions of the loop invariant in terms of the sets  $A_j, B_j$  and  $T_j$ .

**Lemma 1** (Line 4 Loop Invariant). On the  $j$ -th iteration of the **for** loop beginning on line 4, the matrix  $P$  satisfies the following properties:

- (1) If  $P[1, j] \neq 0$  and column  $j$  is indexed by  $\{j_1 \cdots j_k\}$  where  $\{j_1 \cdots j_r\}$  is the longest consecutive set of ascending integers (excluding  $n$ ). Then,

$$P[1, j] = - \left( \sum_{t \in T_j} \text{sgn}(A_j) (-1)^{S_t w_t} \right),$$

and  $P[i : (i + r - 1), j] = \{w_r, \dots, w_1\}$  (the trailing block  $T_j$  for column  $j$ ).

- (2) If  $P[1, j] = 0$ , then either  $\exists$  column  $j'$  such that  $P[1, 1 : (j' - 1)] = 0$  and condition (1) holds for column  $j'$ , or  $i = (2^{n-1} + 1)$ .
- (3) For column  $i$ ,

$$P[1, i] = \sum_{a \in A_i} \text{sgn}(a, A_i) w_a.$$

- (4) For column  $i'$  such that  $i < i'$ , let  $A' \subseteq A_{i'}$ . Then

$$P[1, i'] = \sum_{a \in A'} \text{sgn}(a, A_{i'}) w_a.$$

- (5) For column  $i'$  such that  $j < i' < i$ , let  $B' \subseteq B_{i'}$ . Then

$$P[1, i'] = - \left( \sum_{x \in (T_{i'} \cup B')} \text{sgn}(A_{i'}) (-1)^{S_x w_x} \right).$$

- (6)  $P[1, 1 : (j - 1)] = 0$ .

These loop invariant conditions can be better understood by studying the example displayed in Appendix A, and seeing that each of these conditions hold during each iteration of the algorithm.

*Proof of Lemma 1 (Line 4 Loop Invariant):* We must show that conditions (1) through (6) hold during *initialization*, and are *maintained* from one iteration to another. We must also show that when the FACTORCHECK algorithm terminates, it does so with “useful information”, which in this case is conveyed by condition (6).

**Initialization:**

By Prop. 2, the first  $n$  rows and columns of  $\text{Part}_n$  are always the following:

$$\begin{bmatrix} w_n & w_{n-1} & w_{n-2} & \cdots & w_1 \\ w_{n-1} & w_n & 0 & \cdots & 0 \\ w_{n-2} & 0 & w_n & 0 & \vdots \\ \vdots & \vdots & \ddots & \ddots & 0 \\ w_1 & 0 & \cdots & 0 & w_n \end{bmatrix}$$

Upon initialization of line 4, column  $j = 1$ , row  $i = 2$ , and the substitution

$$w_n = -\left(\sum_{i=1}^{n-1} (-1)^{S_i} w_i\right)$$

has been performed in the matrix  $P$ . We will investigate each of the conditions of Lemma 1, and show that they are true.

- (1) Upon initialization,  $P[1, 1] \neq 0$ , and  $P[2 : n, 1] = \{w_{n-1}, \dots, w_1\}$ . Since there are *no* entries above the diagonal in column 1,  $\text{sgn}(A_j) = 1$ . Therefore, the trailing block  $T_1 = \{w_{n-1}, \dots, w_1\}$ , and

$$P[1, 1] = -\left(\sum_{t \in T_j} (-1)^{S_t} w_t\right),$$

and condition (1) of Lemma 1 holds.

- (2) Since  $P[1, 1] \neq 0$ , condition (2) does not apply.  
(3) For column  $i = 2$ , the entries above the diagonal are  $A_2 = w_{n-1}$ . Therefore,  $\text{sgn}(a, A_i) = 1$  since  $A_i \setminus w_{n-1} = \emptyset$ . Therefore,

$$P[1, i] = \sum_{a \in A_i} \text{sgn}(a, A_i) w_a = w_{n-1},$$

and condition (3) holds.

- (4) For columns  $i' = 3, \dots, n$ , the sets of entries above the diagonal are  $\{w_{n-2}\}, \dots, \{w_1\}$  respectively. Thus  $\text{sgn}(a, A_{i'}) = 1$  since  $A_{i'} \setminus w_a = \emptyset$ , as before. Furthermore, by Prop. 1, there is exactly one entry for each  $w_i$  in a given row. Therefore, the entries in row 1 for columns  $i' = n+1, \dots, 2^{n-1}$  are zero. Therefore, condition (4) holds.  
(5) There are no columns that satisfy  $j < i' < i$  when  $j = 1$  and  $i = 2$ .  
(6) There are no columns less than  $j$  when  $j = 1$ .

Thus, conditions 1 through 6 hold upon initialization. We will now show that each of the conditions are maintained from one iteration to the next.

### Maintenance:

In order to prove *maintenance*, we assume conditions (1) through (6) hold at the  $j$ -th iteration, and we must show that conditions (1) through (6) hold at the  $j+1$ -th iteration. But whether or not the conditions hold depend solely on whether or not lines 6-9 in the inner **while** loop are executed. Thus, we break the proof of maintenance into two cases. The **first** case is when  $P[1, j] = 0$  (when lines 6-9 are *not* executed), and the **second** is when  $P[1, j] \neq 0$  (when lines 6-9 *are* executed).

**Case 1:**  $P[1, j] = 0$ . In this case, lines 6-9 are not executed. Thus, the matrix does not

change between the  $j$ -th and  $(j+1)$ -th iteration. Furthermore, since  $P[1, 1 : (j-1)] = 0$  (condition 6) and  $P[1, j] = 0$ , columns  $P[1, 1 : (j+1)] = 0$ . Finally, by Prop. 4.3, either  $i = 2^{n+1} + 1$ , and we have already cancelled *all* the entries (see the second-to-last step of the example in Appendix A), or there is a column  $j'$  where the trailing block begins at row  $i$ . Thus, the conditions hold at the  $(j+1)$ -th iteration.

**Case 2:**  $P[1, j] \neq 0$ . In this case, lines 6-9 are executed. Furthermore, by condition (1),  $P[i : (i+r-1), j] = \{w_r, \dots, w_1\}$ . Since

$$P[1, j] = - \left( \sum_{t \in T_j} \text{sgn}(A_j)(-1)^{S_t} w_t \right),$$

the signs calculated in line 7 during the  $j$ -th iteration are

$$(\text{sgn}(A_j)(-1)^{S_r}), (\text{sgn}(A_j)(-1)^{S_{r-1}}) \dots, (\text{sgn}(A_j)(-1)^{S_1}).$$

Thus, after the  $r$  iterations of the **while** loop of line 5, the entries  $w_r, \dots, w_1$  present in  $P[1, j]$  will be cancelled, and  $P[1, j] = 0$ . Therefore,  $P[i, 1 : j] = 0$  at the beginning of the  $(j+1)$ -th iteration, and condition (6) of the loop invariant holds.

Now we consider an arbitrary row operation performed in line 8, and assume that conditions (3) through (5) hold *before* the operation, and prove that the conditions hold *after* the operation. Let  $i_t$  be an arbitrary row with  $i \leq i_t \leq (i+r-1)$  and  $P[i_t, j] = w_t$ . Since we have already shown that the conditions hold on column  $j$ , we must only consider the effect of this operation on entries to the *left* of the diagonal ( $j < i' < i_t$ ), the diagonal ( $i' = i_t$ ), and the *right* of the diagonal ( $i_t < i'$ ).

- ( $j < i' < i_t$ ): Consider a non-zero entry  $P[i_t, i'] = w_b$ , with  $j < i' < i_t$  (an entry to the *left* of the diagonal). By the loop invariant,

$$P[1, i'] = - \left( \sum_{x \in (T_{i'} \cup B')} \text{sgn}(A_{i'})(-1)^{S_x} w_x \right).$$

The row operation performed is  $\text{sgn}(A_j)(-1)^{S_t} P[i_t, i'] + P[1, i']$ . However, by Prop. 6,  $A_j \cup P[i_t, j] = A_{i'} \cup P[i_t, i']$ . Therefore,  $w_b \in A_j$  and  $w_t \in A_{i'}$ . In particular,  $\text{sgn}(A_j)(-1)^{S_t} = \text{sgn}(A_{i'})(-1)^{S_b}$ . Since the sign of  $w_b$  in  $P[1, i']$  is equal to  $-(\text{sgn}(A_{i'})(-1)^{S_b})$ , this row operation *cancels the entry  $w_b$  in  $P[1, i']$* , and condition (5) of the loop invariant holds. Moreover, we observe that, in the case where  $i' = j+1$ , then every entry above the trailing block has been iterated, and therefore cancelled. Thus, either  $P[1, j+1] = 0$  (if there is no trailing block), or every entry in  $B_{j+1}$  has been canceled and

$$P[1, j+1] = - \left( \sum_{t \in T_{j+1}} \text{sgn}(A_{j+1})(-1)^{S_t} w_t \right).$$

Thus, we have shown that when  $j < i' < i_t$ , all relevant conditions of the loop invariant hold.

- ( $i' = i_t$ ): Now, we will consider the row operation performed on the diagonal, or  $\text{sgn}(A_j)(-1)^{S_t} P[i_t, i_t] + P[1, i_t]$ . By condition (3) of the loop invariant,

$$P[1, i_t] = \sum_{a \in A_{i_t}} \text{sgn}(a, A_{i_t}) w_a.$$

But, by Prop 5, we know that the entries in row  $i_t$  between columns  $j$  and  $i_t$  (excluding  $P[i_t, j]$ ) are the *same* as the entries above the diagonal in column  $j$ . Furthermore, by the symmetry of the matrix (Prop 3.6), we know that  $P[i_t, 1 : i_t] = P[1 : i_t, i_t]$ . Thus, the entries above the diagonal in column  $i_t$  are the *same* as the entries  $P[i_t, j] \cup A_j$ . Thus,  $\text{sgn}(A_j)(-1)^{S_i} = \text{sgn}(A_{i_t})$ . Recall also, that since  $P[i_t, i_t]$  is a diagonal element,

$$P[i_t, i_t] = - \left( \sum_{i=1}^{n-1} (-1)^{S_i} w_i \right)$$

Consider a particular  $w_a \in P[i_t, i_t]$  such that  $a \in A_{i_t}$ . Then, the sign of  $w_a$  in  $P[i_t, i_t]$  is  $-((-1)^{S_a})$ . But

$$-((-1)^{S_a} \text{sgn}(A_{i_t})) = -((-1)^{S_a} (-1)^{S_a}) \cdot \text{sgn}(a, A_{i_t}) = -\text{sgn}(a, A_{i_t}) .$$

Thus, the row operation  $\text{sgn}(A_j)(-1)^{S_t} P[i_t, i_t] + P[1, i_t]$  cancels *all*  $w_a$  with  $a \in A_{i_t}$ , and

$$P[1, i_t] = - \left( \sum_{x \in (T_{i_t} \cup B_{i_t})} \text{sgn}(A_{i_t})(-1)^{S_x} w_x \right) .$$

Finally, row  $i_t$  is incremented to  $i_t + 1$ , and condition (5) of the loop invariant holds. Thus, when  $i' = i_t$ , all relevant conditions of the loop invariant hold.

- ( $i_t < i'$ ): Finally, consider an entry  $P[i_t, i'] = w_a$ , where  $i_t < i'$  (consider an entry to the *right* of the diagonal). By the loop invariant,

$$P[1, i'] = \sum_{a \in A'} \text{sgn}(a, A_{i'}) w_a ,$$

where  $A' \subseteq A_{i'}$  is a subset of the set of entries above the diagonal in column  $i'$ . The row operation performed is  $\text{sgn}(A_j)(-1)^{S_t} P[i_t, i'] + P[1, i']$ . However, by Prop. 7,  $A_j \cup P[i_t, j] \cup P[i_t, i'] = A_{i'}$ . Therefore,  $w_t \in A_{i'}$ , and  $\text{sgn}(A_j)(-1)^{S_t} = \text{sgn}(a, A_{i'})$ . Moreover, we can be certain that  $a$  is not in the set  $A'$ , since there is exactly one entry per column for each  $a = 1, \dots, n$ , and the only entries in  $A'$  are those that have been added there by previous row operations. Therefore, let  $A' \cup a = A'' \subseteq A_{i'}$ , and after the line 8 row operation,

$$P[1, i'] = \sum_{a \in A''} \text{sgn}(a, A_{i'}) w_a ,$$

and condition (4) of the loop invariant holds. Moreover, when  $i' = i_t + 1$ ,  $A'' = A_{i'}$ , since *every* entry above the diagonal has been added to  $P[1, i']$ . In this case, after  $i_t$  is incremented to  $i_t + 1$  in line 9, condition (3) (the diagonal condition) of the loop invariant holds. Thus, when  $i_t < i'$ , all relevant conditions of the loop invariant hold.

Therefore, we have shown that if conditions (3) through (5) hold at the beginning of the  $j$ -th iteration, an arbitrary iteration of lines 6 – 9 will not alter those conditions. We have therefore shown that if conditions (1) through (6) hold at the  $j$ -th iteration, then conditions (1) through (6) also hold at the  $(j + 1)$ -th iteration.

### Termination:

The last row of  $\text{Part}_n[2^{n-1}, :]$  consists of all zeros, except for the last  $n$  entries. In specific,  $\text{Part}_n[2^{n-1}, 2^{n-1} - n + 1 : 2^{n-1}]$ . Thus, during the iteration when column

$j = 2^{n-1} - n + 1$ , the last row is added to the first row (with the correct signs since the loop invariant is maintained). Thus, during that iteration,  $P[1, :] = 0$ . Thus, when the algorithm terminates, the first row of the output matrix  $P$  consists entirely of zeros. This is the “useful information” that will help us prove our main result.  $\square$

*Proof of Theorem 8:* The determinant of the partition matrix has degree  $2^{n-1}$ . We choose an arbitrary bitstring  $S \in \{0, 1\}^{n-1}$  (which also defines an arbitrary partition of the set  $W$ ), and substitute that factor into the partition matrix (line 2 of the algorithm FACTORCHECK). We have previously shown that the algorithm FACTORCHECK terminates with an output matrix  $P$  where the first row consists entirely of zeros. Therefore, the determinant of the output matrix  $P$  is zero, and the substitution performed in line 2 is a root of the determinant. Since the input factor defined by the bitstring  $S$  in the FACTORCHECK algorithm is an arbitrary factor, and an arbitrary partition, we have shown that *any* factor  $S$  has the same result. Since every factor is a root, and there are  $2^{n-1}$  factors and only  $2^{n-1}$  roots of the determinant, the determinant of the partition matrix is the partition polynomial.  $\square$

## Acknowledgements

The authors would like to acknowledge the support of NSF DSS-0729251, NSF-CSSI-0926618, DSS-0240058, the Rice University VIGRE program, and the Defense Advanced Research Projects Agency under Award No. N66001-10-1-4040. Additionally, research on this projected was supported in part by a grant from the Israel Science Foundation.

## References

- [1] N. Alon, Combinatorial Nullstellensatz, *Combinatorics, Probability and Computing*, 8:7–29, 1992.
- [2] N. Alon and S. Tarsi, Colorings and orientations of graphs, *Combinatorica*, 12:125–134, 1992.
- [3] E. Babson, S. Onn and R.R. Thomas, The Hilbert zonotope and a polynomial time algorithm for universal Gröbner bases, *Advances in Applied Mathematics*, 30:529–544, 2003.
- [4] S. Buss and T. Pitassi, Good degree bounds on Nullstellensatz refutations of the induction principle, *IEEE Conference on Computational Complexity*, 233–242, 1996.
- [5] D. Cox and J. Little and D. O’Shea, Ideals, Varieties and Algorithms, *Springer*, New York, 1998.
- [6] J.A. De Loera, J. Lee, P.N. Salkin, S. Margulies, Computing Infeasibility Certificates for Combinatorial Problems through Hilbert’s Nullstellensatz, *Journal of Symbolic Computation*, 46(11), pg. 1260-1283, 2011.
- [7] J.A. De Loera, J. Lee, P.N. Salkin, S. Margulies, Hilbert’s Nullstellensatz and an Algorithm for Proving Combinatorial Infeasibility, Internatl. Symposium on Symbolic and Algebraic Computation, ISSAC 2009.
- [8] J. De Loera, J. Lee, S. Margulies and S. Onn, Expressing combinatorial optimization problems by systems of polynomial equations and the Nullstellensatz, *Combinatorics, Probability and Computing*, 18:551–582, 2009.

- [9] S. Garey and D. Johnson, Computers and Intractability: A Guide to the Theory of NP-Completeness, *W.H. Freeman and Company*, 1979.
- [10] L. Lovász, Stable sets and Polynomials, *Discrete Mathematics*, 124:137–153, 1994.
- [11] S. Margulies, Computer Algebra, Combinatorics and Complexity Theory: Hilbert’s Nullstellensatz and NP-complete problems. Ph.D. thesis, UC Davis, 2008.
- [12] S. Onn, Nowhere-zero flow polynomials, *Journal of Combinatorial Theory Series A*, 108:205–215, 2004.

## A. Appendix

Here we display the FACTORCHECK algorithm running step-by-step input  $n = 4$  and factor  $(-w_1 - w_2 + w_3 + w_4)$ , described by bitstring  $S = 1100$ . Below follows  $P = \text{Part}_4$  on line 1 of FACTORCHECK:

$$P = \begin{array}{c|cccccccc} & 123 & 124 & 134 & 234 & 1 & 2 & 3 & 4 \\ \hline 1234 & w_4 & w_3 & w_2 & w_1 & 0 & 0 & 0 & 0 \\ 12 & w_3 & w_4 & 0 & 0 & w_2 & w_1 & 0 & 0 \\ 13 & w_2 & 0 & w_4 & 0 & w_3 & 0 & w_1 & 0 \\ 23 & w_1 & 0 & 0 & w_4 & 0 & w_3 & w_2 & 0 \\ 14 & 0 & w_2 & w_3 & 0 & w_4 & 0 & 0 & w_1 \\ 24 & 0 & w_1 & 0 & w_3 & 0 & w_4 & 0 & w_2 \\ 34 & 0 & 0 & w_1 & w_2 & 0 & 0 & w_4 & w_3 \\ \emptyset & 0 & 0 & 0 & 0 & w_1 & w_2 & w_3 & w_4 \end{array}.$$

Below follows  $P$  on line 4, after the substitution  $w_4 = w_1 + w_2 - w_3$ , with column  $j = 1$  and row  $i = 2$ . During this iteration of the **for** loop, we perform row operations  $P[1, :] = P[2, :] + P[1, :]$ ,  $P[1, :] = -P[3, :] + P[1, :]$ , and  $P[1, :] = -P[4, :] + P[1, :]$ .

$$\begin{array}{c|cccccccc} & 123 & 124 & 134 & 234 & 1 & 2 & 3 & 4 \\ \hline 1234 & w_1 + w_2 - w_3 & w_3 & w_2 & w_1 & 0 & 0 & 0 & 0 \\ 12 & w_3 & w_1 + w_2 - w_3 & 0 & 0 & w_2 & w_1 & 0 & 0 \\ 13 & w_2 & 0 & w_1 + w_2 - w_3 & 0 & w_3 & 0 & w_1 & 0 \\ 23 & w_1 & 0 & 0 & w_1 + w_2 - w_3 & 0 & w_3 & w_2 & 0 \\ 14 & 0 & w_2 & w_3 & 0 & w_1 + w_2 - w_3 & 0 & 0 & w_1 \\ 24 & 0 & w_1 & 0 & w_3 & 0 & w_1 + w_2 - w_3 & 0 & w_2 \\ 34 & 0 & 0 & w_1 & w_2 & 0 & 0 & w_1 + w_2 - w_3 & w_3 \\ \emptyset & 0 & 0 & 0 & 0 & w_1 & w_2 & w_3 & w_1 + w_2 - w_3 \end{array}.$$

Below follows  $P$  on line 4 with column  $j = 2$  and row  $i = 5$ . Here we perform the row operations  $P[1, :] = -P[5, :] + P[1, :]$  and  $P[1, :] = -P[6, :] + P[1, :]$ .

$$\begin{array}{c|cccccccc} & 123 & 124 & 134 & 234 & 1 & 2 & 3 & 4 \\ \hline 1234 & 0 & w_1 + w_2 & -w_1 + w_3 & -w_2 + w_3 & -w_3 + w_2 & w_1 - w_3 & -w_1 - w_2 & 0 \\ 12 & w_3 & w_1 + w_2 - w_3 & 0 & 0 & w_2 & w_1 & 0 & 0 \\ 13 & w_2 & 0 & w_1 + w_2 - w_3 & 0 & w_3 & 0 & w_1 & 0 \\ 23 & w_1 & 0 & 0 & w_1 + w_2 - w_3 & 0 & w_3 & w_2 & 0 \\ 14 & 0 & w_2 & w_3 & 0 & w_1 + w_2 - w_3 & 0 & 0 & w_1 \\ 24 & 0 & w_1 & 0 & w_3 & 0 & w_1 + w_2 - w_3 & 0 & w_2 \\ 34 & 0 & 0 & w_1 & w_2 & 0 & 0 & w_1 + w_2 - w_3 & w_3 \\ \emptyset & 0 & 0 & 0 & 0 & w_1 & w_2 & w_3 & w_1 + w_2 - w_3 \end{array}.$$

Below follows  $P$  on line 4 with column  $j = 3$  and row  $i = 7$ . During this iteration of the **for** loop, we perform the single row operation  $P[1, :] = P[7, :] + P[1, :]$ , which cancels *both* columns 3 and 4, row 1.

	123	124	134	234	1	2	3	4
1234	0	0	$-w_1$	$-w_2$	$-w_1$	$-w_2$	$-w_1 - w_2$	$-w_1 - w_2$
12	$w_3$	$w_1 + w_2 - w_3$	0	0	$w_2$	$w_1$	0	0
13	$w_2$	0	$w_1 + w_2 - w_3$	0	$w_3$	0	$w_1$	0
23	$w_1$	0	0	$w_1 + w_2 - w_3$	0	$w_3$	$w_2$	0
14	0	$w_2$	$w_3$	0	$w_1 + w_2 - w_3$	0	0	$w_1$
24	0	$w_1$	0	$w_3$	0	$w_1 + w_2 - w_3$	0	$w_2$
34	0	0	$w_1$	$w_2$	0	0	$w_1 + w_2 - w_3$	$w_3$
$\emptyset$	0	0	0	0	$w_1$	$w_2$	$w_3$	$w_1 + w_2 - w_3$

Below follows  $P$  on line 4 with column  $j = 5$  and row  $i = 8$ . During this iteration of the **for** loop, we perform the single row operation  $P[1, :] = P[7, :] + P[1, :]$ , which cancels *all* the rest of the columns.

	123	124	134	234	1	2	3	4
1234	0	0	0	0	$-w_1$	$-w_2$	$-w_3$	$-w_1 - w_2 + w_3$
12	$w_3$	$w_1 + w_2 - w_3$	0	0	$w_2$	$w_1$	0	0
13	$w_2$	0	$w_1 + w_2 - w_3$	0	$w_3$	0	$w_1$	0
23	$w_1$	0	0	$w_1 + w_2 - w_3$	0	$w_3$	$w_2$	0
14	0	$w_2$	$w_3$	0	$w_1 + w_2 - w_3$	0	0	$w_1$
24	0	$w_1$	0	$w_3$	0	$w_1 + w_2 - w_3$	0	$w_2$
34	0	0	$w_1$	$w_2$	0	0	$w_1 + w_2 - w_3$	$w_3$
$\emptyset$	0	0	0	0	$w_1$	$w_2$	$w_3$	$w_1 + w_2 - w_3$

Finally, below follows  $P$  upon termination. Notice that the first row of the matrix consists entirely of zeros, proving that this factor is a root of the determinant.

	123	124	134	234	1	2	3	4
1234	0	0	0	0	0	0	0	0
12	$w_3$	$w_1 + w_2 - w_3$	0	0	$w_2$	$w_1$	0	0
13	$w_2$	0	$w_1 + w_2 - w_3$	0	$w_3$	0	$w_1$	0
23	$w_1$	0	0	$w_1 + w_2 - w_3$	0	$w_3$	$w_2$	0
14	0	$w_2$	$w_3$	0	$w_1 + w_2 - w_3$	0	0	$w_1$
24	0	$w_1$	0	$w_3$	0	$w_1 + w_2 - w_3$	0	$w_2$
34	0	0	$w_1$	$w_2$	0	0	$w_1 + w_2 - w_3$	$w_3$
$\emptyset$	0	0	0	0	$w_1$	$w_2$	$w_3$	$w_1 + w_2 - w_3$